In the Claims:

Claims 1-25 (Canceled).

26. (Currently Amended) <u>A system for providing continuous authentication of a user of a computing device, comprising:</u>

<u>a security component which provides security functions, such that the security component can vouch for authenticity of one or more other components with which it is securely operably connected;</u>

<u>a biometric sensor component that is securely operably connected, as one of the one or more other components, to the security component;</u>

<u>securely-stored biometric information which identifies an owner of the computing device;</u>

<u>means for repeatedly obtaining, from the biometric sensor component, biometric input of a user of the computing device, wherein the means for repeatedly obtaining is activated upon beginning a security-sensitive operation and is terminated upon completion of the security-sensitive operation;</u>

<u>means for comparing the repeatedly obtained biometric input to the securely-stored biometric information of the owner, wherein each of the comparisons comprises an authentication of the user; and</u> ~~The system according to Claim 25, wherein the~~

means for concluding, <u>within a security core,</u> that the security-sensitive operation is authentic ~~also requires that~~ <u>based on</u> all other components which are securely operably connected to the security core ~~remain~~ <u>remaining</u> securely operably connected until completion of the security-sensitive operation.

27. (Currently amended) <u>A system for providing continuous authentication of a user of a computing device, comprising:</u>

<u>a security component which provides security functions, such that the security component can vouch for authenticity of one or more other components with which it is securely operably connected;</u>

<u>a biometric sensor component that is securely operably connected, as one of the one or more other components, to the security component;</u>

securely-stored biometric information which identifies an owner of the computing device;

means for repeatedly obtaining, from the biometric sensor component, biometric input of a user of the computing device, wherein the means for repeatedly obtaining is activated upon beginning a security-sensitive operation and is terminated upon completion of the security-sensitive operation;

means for comparing the repeatedly obtained biometric input to the securely-stored biometric information of the owner, wherein each of the comparisons comprises an authentication of the user; and ~~The system according to Claim 25, wherein the~~

means for concluding, within a security core, that the security-sensitive operation is authentic ~~also requires that~~ based on all other components which are securely operably connected to the security core and which are involved in the security-sensitive operation ~~remain~~ remaining securely operably connected until completion ~~thereof~~ of the security-sensitive operation.

Claims 28-59 (Canceled).

60.   (Currently amended) A method for providing continuous authentication of a user of a computing device, comprising:

operating a security component which provides security functions, such that the security component can vouch for authenticity of one or more other components with which it is securely operably connected;

providing a biometric sensor component that is securely operably connected, as one of the one or more other components, to the security component;

providing securely-stored biometric information which identifies an owner of the computing device;

repeatedly obtaining, from the biometric sensor component, biometric input of a user of the computing device, wherein the repeatedly obtaining is activated upon beginning a security-sensitive operation and is terminated upon completion of the security-sensitive operation;

comparing the repeatedly obtained biometric input to the securely-stored biometric information of the owner, wherein each of the comparisons comprises an authentication of the user; and ~~The method according to Claim 59, wherein the step of~~

concluding with a security core that the security-sensitive operation is authentic ~~also~~ ~~requires that~~ based on all other components which are securely operably connected to the security core ~~remain~~ remaining securely operably connected until completion of the security-sensitive operation.

61. (Currently amended) A method for providing continuous authentication of a user of a computing device, comprising:

operating a security component which provides security functions, such that the security component can vouch for authenticity of one or more other components with which it is securely operably connected;

providing a biometric sensor component that is securely operably connected, as one of the one or more other components, to the security component;

providing securely-stored biometric information which identifies an owner of the computing device;

repeatedly obtaining, from the biometric sensor component, biometric input of a user of the computing device, wherein the repeatedly obtaining is activated upon beginning a security-sensitive operation and is terminated upon completion of the security-sensitive operation;

comparing the repeatedly obtained biometric input to the securely-stored biometric information of the owner, wherein each of the comparisons comprises an authentication of the user; and ~~The method according to Claim 59, wherein the step of~~

concluding within a security core that the security-sensitive operation is authentic ~~also~~ ~~requires that~~ based on all other components which are securely operably connected to the security core and which are involved in the security-sensitive operation ~~remain~~ remaining securely operably connected until completion thereof.

Claims 62-93 (Canceled).

94.   (Currently amended) <u>A computer program product for providing continuous</u> <u>authentication of a user of a computing device, the computer program product embodied on</u> <u>one or more computer-readable media and comprising:</u>

<u>computer-readable program code that is configured to operate a security component</u> <u>which provides security functions, such that the security component can vouch for</u> <u>authenticity of one or more other components with which it is securely operably connected;</u>

<u>computer-readable program code that is configured to access a biometric sensor</u> <u>component that is securely operably connected, as one of the one or more other components,</u> <u>to the security component;</u>

<u>computer-readable program code that is configured to access securely-stored</u> <u>biometric information which identifies an owner of the computing device;</u>

<u>computer-readable program code that is configured to repeatedly obtain, from the</u> <u>biometric sensor component, biometric input of a user of the computing device, and to be</u> <u>activated upon beginning a security-sensitive operation and terminated upon completion of</u> <u>the security-sensitive operation;</u>

<u>computer-readable program code that is configured to compare the repeatedly</u> <u>obtained biometric input to the securely-stored biometric information of the owner, wherein</u> <u>each of the comparisons comprises an authentication of the user; and</u> ~~The computer program~~ ~~product according to Claim 93, wherein the~~

computer-readable program code ~~means for concluding~~ <u>that is configured to conclude</u> <u>within a security core</u> that the security-sensitive operation is authentic ~~also requires that~~ <u>based</u> <u>on</u> all other components which are securely operably connected to the security core ~~remain~~ <u>remaining</u> securely operably connected until completion of the security-sensitive operation.

95.   (Currently amended) <u>A computer program product for providing continuous</u> <u>authentication of a user of a computing device, the computer program product embodied on</u> <u>one or more computer-readable media and comprising:</u>

<u>computer-readable program code that is configured to operate a security component</u> <u>which provides security functions, such that the security component can vouch for</u> <u>authenticity of one or more other components with which it is securely operably connected;</u>

computer-readable program code that is configured to access a biometric sensor

component that is securely operably connected, as one of the one or more other components,

to the security component;

computer-readable program code that is configured to access securely-stored

biometric information which identifies an owner of the computing device;

computer-readable program code that is configured to repeatedly obtain, from the

biometric sensor component, biometric input of a user of the computing device, and to be

activated upon beginning a security-sensitive operation and terminated upon completion of

the security-sensitive operation;

computer-readable program code that is configured to compare the repeatedly

obtained biometric input to the securely-stored biometric information of the owner, wherein

each of the comparisons comprises an authentication of the user; and ~~The computer program~~

~~product according to Claim 93, wherein the~~

computer-readable program code ~~means for concluding~~ that is configured to conclude

within a security core that the security-sensitive operation is authentic ~~also requires that~~ based

on all other components which are securely operably connected to the security core and

which are involved in the security-sensitive operation ~~remain~~ remaining securely operably

connected until completion thereof.

Claims 96-102 (Canceled).

103.   (Currently amended) A method of doing business by continually

authenticating a user of a computing device, comprising ~~steps of~~:

operating a security component for the computing device, wherein the security

component provides security functions such that the security component can vouch for

authenticity of one or more other components with which it is securely operably connected;

providing a biometric sensor component that is securely operably connected, as one of

the one or more other components, to the security component;

providing securely-stored biometric information which identifies an owner of the

computing device;

performing a security-sensitive operation using the computing device;

repeatedly obtaining, from the biometric sensor component, biometric input of a user of the computing device over a duration of the security-sensitive operation;

comparing the repeatedly obtained biometric input to the securely-stored biometric information of the owner, wherein each of the comparisons comprises an authentication of the user;

determining within a security core that the security-sensitive operation is authentic based on all other components which are securely operably connected to the security core and which are involved in the security-sensitive operation remaining securely operably connected until completion of the security-sensitive operation; and

aborting the security-sensitive operation if the comparing step fails at any time over the duration of the security-sensitive operation or if the security-sensitive operation is determined not to be authentic.

104.   (Currently amended) A method of improving security of a computing device, comprising steps of:

operating a security component for the computing device, wherein the security component provides security functions such that the security component can vouch for authenticity of one or more other components with which it is securely operably connected;

providing a biometric sensor component that is securely operably connected, as one of the one or more other components, to the security component;

providing securely-stored biometric information which identifies an owner of the computing device;

repeatedly obtaining, from the biometric sensor component, biometric input of a user of the computing device; and

comparing the repeatedly obtained biometric input to the securely-stored biometric information of the owner;

performing a security-sensitive operation using the computing device; and

determining within a security core that the security-sensitive operation is authentic based on all other components which are securely operably connected to the security core and which are involved in the security-sensitive operation remaining securely operably connected until completion of the security-sensitive operation.

105. (Currently amended) A method of improving security of operations carried out with a computing device, comprising ~~steps of~~:

operating a security component for the computing device, wherein the security component provides security functions such that the security component can vouch for authenticity of one or more other components with which it is securely operably connected;

providing a biometric sensor component that is securely operably connected, as one of the one or more other components, to the security component;

providing securely-stored biometric information which identifies an owner of the computing device;

performing a security-sensitive operation using the computing device;

repeatedly obtaining, from the biometric sensor component, biometric input of a user of the computing device over a duration of the security-sensitive operation;

comparing the repeatedly obtained biometric input to the securely-stored biometric information of the owner, wherein each of the comparisons comprises an authentication of the user; and

<u>determining within a security core that the security-sensitive operation is authentic based on all other components which are securely operably connected to the security core and which are involved in the security-sensitive operation remaining securely operably connected until completion of the security-sensitive operation</u>

~~aborting the security-sensitive operation if the comparing step fails at any time over the duration of the security-sensitive operation~~.